Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ

Комп’ютерний практикум №2

«Криптоаналіз шифру Віженера»

Варіант №2

Виконали:

студенти групи ФБ-93

Бурячок А.А

Данілін Д.Д.

Перевірила:

Селюх П.В.

Київ - 2021

Мета: засвоєння методів часткового криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Завдання:

- уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини , а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
- підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
- використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (варіант №2).

Хід роботи:

Частина 1

Обираємо довільний текст, довжиною 2-3 Кб. Відформатований текст, у якому видалені пробіли на замінено літеру 'ё' на 'е' знаходиться у файлі text.txt. Генеруємо випадкові ключі довжиною 2-5 та 10-20 символів. Для шифрування та дешифрування використовуємо написані нами функції encrypt та decrypt, які приймають в якості аргументу текст, який потрібно зашифрувати чи розшифрувати відповідно, та сам ключ.

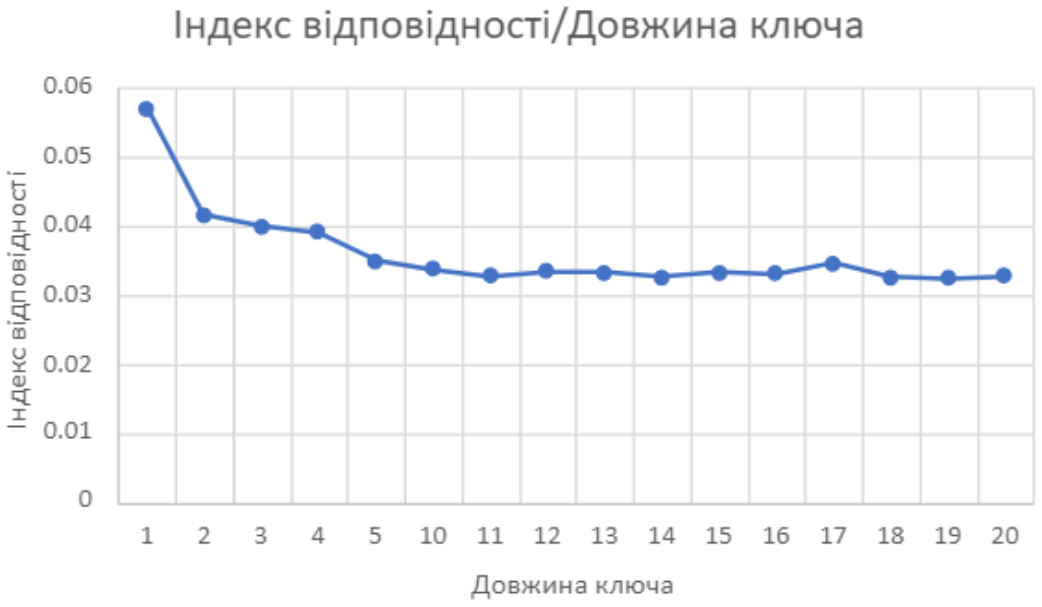
Частина 2

Обчислюємо індекси відкритого та шифрованих текстів відповідними ключами. Таблиця з усіма результатами наведена нижче.

Довжина	Ключ	Індекс відповідності
-	-	0.0570476
2	па	0.0416642
3	твр	0.0400618

4	ънот	0.0391597
5	яэгжн	0.0350196
10	цпукснфщих	0.0338872
11	уърьбеоахзр	0.0327704
12	мябыьщуевяъд	0.0335141
13	ибчжчцтгчфяпш	0.0332421
14	эафсылазрнырзп	0.0325585
15	ьшпшьгйфлфафбощ	0.0333381
16	хшщлеширгушьзуыо	0.0331340
17	врцезжзфкжмщзмалж	0.0345634
18	сзтювмышсимцкжхуйе	0.0326932
19	имкюкабжкфлцсъдйытъ	0.0324271
20	жесвязвкщелпнасротюв	0.0327391

На діаграмі нижче можна перевірити той факт, що при збільшенні довжини ключа зменшується індекс відповідності.



Частина 3

Підбираємо довжину ключа, для цього обчислюємо середнє значення індексу відповідності. Таблиця з результатами наведена нижче.

Довжина ключа	Індекс відповідності	Довжина ключа	Індекс відповідності
1	0.0348578	11	0.0348727
2	0.0362682	12	0.0362870
3	0.0348277	13	0.0348809
4	0.0363681	**14**	**0.0552817**
5	0.0349229	15	0.0349050
6	0.0362575	16	0.0363696
7	0.0446260	17	0.0348421
8	0.0364226	18	0.0362361
9	0.0347582	19	0.0348722
10	0.0362297	20	0.0361005

Як можна побачити, при довжині ключа 14 індекс відповідності різко збільшується. При цьому значення індексу відповідності для дільників 14 (тобто 2 та 7) не приймають таких великих значень. Отже, можна прийти до висновку, що довжина ключа, яким був зашифрований текст дорівнює 14.

Перевіримо цей факт за допомогою методу, який базується на обчисленні статистики збігів символів. Таблиця з результатами наведена нижче.

Довжина ключа	Статистика збігів	Довжина ключа	Статистика збігів
1	239	11	247
2	258	12	247
3	236	13	212
4	262	**14**	**396**
5	240	15	252
6	232	16	253
7	244	17	262

8	220	18	252
9	238	19	247
10	253	20	233

Як можна помітити, при довжині ключа 14 маємо різке збільшення статистики збігів символів, а на дільниках 14 такого явища не було. Отже, ми впевнилися, що довжина ключа дійсно дорівнює 14.

Якщо ми знаємо довжину ключа при шифруванні шифром Віженера, то розшифрування зводится до розшифрування n шифрів Цезаря, де n - довжина ключа. Для цього використовуємо частотний аналіз, який допоможе знайти символ у блоці, який зустрічається найбільшу кількість разів. Таблиця з результатами наведена нижче.

Блок	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Символ	ф	ь	я	р	у	й	т	ц	о	т	ь	х	ь	ю

Тепер потрібно знайти символи ключа, для цього віднімаємо від найчастішого символу найочікуваніший символ тексту (літери ‘о’, ‘а’, ‘е’). Отримуємо декілька варіантів ключів. Таблиця з результатами наведена нижче.

Символ	Ключ
о	**жосве**ыд**иадозор**
е	**п**чъ**лоднсй**нчрчщ
а	фьяруйтцотьхью

Після отримання розшифрованого тексту ключем “жосвеыдиадозор”, ми отримали нечитабельний текст. Тому ми почали шукати помилки у знайомих нам словах. Так ми помітили, що справжній ключ був комбінацією ключів з найчастішими літерами ‘о’ та ‘е’. В результаті ми отримати наступний ключ, яким був зашифрований текст: “последнийдозор”. Відкритий текст, який ми отримали знаходиться у файлі result.txt.

Висновки: в ході лабораторної роботи ми вивчили методи часткового криптоаналізу, здобули навички щодо роботи та аналізу шифрів гамування адитивного типу, дослідили те, як поводять себе індекси відповідності та

статистика збігів символів при різних довжинах ключа, на основі цих даних змогли розшифрувати текст, який був зашифрований шифром Віженера.